

BEST AVAILABLE COPY

(19) 대한민국특허청 (KR)
(12) 특허공보(B1)

USP 5,341,422

(51) Int. ⁶ Cl.		(11) 등록번호	특 1997-0006392
G06F 1 /00		(24) 등록일자	1997년04월28일
(21) 출원번호	특1993-0018645	(65) 공개번호	특1994-0007674
(22) 출원일자	1993년09월14일	(43) 공개일자	1994년04월27일
(30) 우선권 주장	947,014 1992년09월17일 미국(US)		
(73) 특허권자	인터내셔널 비지네스 머신즈 코포레이션	윌리엄 티. 엘리스	
(72) 발명자	미합중국 뉴욕 10504 아몬크 존 월레이 블랙크레지 2세 미합중국 플로리다 33487 보카 라톤 세쿼이아스 레인 304 리차드 알란 다이안 미합중국 플로리다 33487 보카 라톤 노오스이스트 73 스트리트 830 데니스 리 모엘럴 미합중국 플로리다 33487 보카 라톤 로스우드 설클 7430 팔말 유겐 뉴맨 미합중국 플로리다 33433 보카 라톤 돌빈 드라이브 7488 켄네스 제이. 피. 주베이 미합중국 플로리다 33433 보카 라톤 아이언위치 드라이브 22845		
(74) 대리인	김창세, 장성구		
심사관 : 홍순우 (특자공보 제4973호)			
(54) 보안 기능을 갖는 퍼스널 컴퓨터 시스템.			

요약

내용없음.

대표도

도1

명세서

[발명의 명칭]

보안 기능을 갖는 퍼스널 컴퓨터 시스템

[도면의 간단한 설명]

제1도는 본 발명을 구현하는 퍼스널 컴퓨터 시스템의 사시도.

제2도는 사시, 덮개와 플래너 보드를 포함하는(제1도의) 퍼스널 컴퓨터의 어떤 요소들의 분해사시도(이들 요소들간의 관계를 나타냄).

제3도는 제1도 및 제2도에 도시된 퍼스널 컴퓨터의 어떤 구성 요소들의 개략도.

제4도 및 제5도는 본 발명의 보안기능에 관계되는 제1도 및 제2도의 퍼스널 컴퓨터의 어떤 구성요소들을 나타내는 개략도

제6도는 제4도 및 제5도에 도시된 어떤 구성요소들의 확대 사시도.

제7도는 본 발명의 보안기능에 관계되는 제1, 2, 4도 및 제5도에 도시된 퍼스널 컴퓨터의 특정의 선택사양적인 구성요소들을 나타내는, 제6도와 유사한 도면.

* 도면의 주요부분에 대한 부호의 설명

10 : 컴퓨터	11 : 모니터
12 : 키보드	14 : 프린터 또는 플러터
15 : 덮개	10 : 사시
20 : 플레이너	22 : 상부베어

[발명의 상세한 설명]

본 발명은 퍼스널 컴퓨터 시스템(personal computer system)에 관한 것으로서, 특히, 퍼스널 컴퓨터 시스템이 보유한 데이터에 대한 액세스(access)를 제어할 수 있는 보안기능(security feature)을 구비한 퍼스널 컴퓨터 시스템에 관한 것이다.

일반적으로 퍼스널 컴퓨터 시스템, 특히 IBM 퍼스널 컴퓨터 시스템은 오늘날 현대 사회의 많은 부분에 컴퓨터 파워(computer power)를 제공하는 용도로 널리 보급되어 왔다. 퍼스널 컴퓨터 시스템은 단일 시스템 프로세서와, 시스템 프로세서와 관련된 휘발성(volatile) 및 비휘발성(non-volatile)메모리, 디스플레이 모니터, 키보드, 하나 또는 그 이상의 디스켓 구동기(diskette drives), 고정 디스크 기억장치 및 선택사양적 프린터를 갖춘 시스템 유닛으로 구성된 데스크-탑(desk-top), 플로어 스탠딩(floor standing) 또는 휴대용 마이크로 컴퓨터로 정의된다. 이러한 장치들의 두드러진 특징 중의 하나는 이들 구성요소를 서로 전기적으로 연결하는 마더보드(motherboard)(시스템 보드(system board), 시스템 플래너(system planar) 또는 플래너(planar)로 알려져 있으며 본 명세서에서는 경우에 따라 이러한 용어로도 지칭한다)를 사용하는 것이다. 이러한 시스템들은 주로 한명의 사용자에게 독자적인 계산능력을 제공하도록 설계되고 개인 또는 소규모 사업자가 구입할 수 있게 저렴한 가격으로 공급된다. 이러한 퍼스널 컴퓨터 시스템의 예는 IBM의 퍼스널 컴퓨터 AT(PERSONAL COMPUTER AT)와 IBM의 퍼스널 시스템/2(PERSONAL SYSTEM/2)모델들 25, 30, 35, 40, L40SX, 50, 55, 57, 65, 70, 80, 90과 95이다.

이러한 시스템들은 2개의 일반적 패밀리들(families)로 분류될 수 있다. 통상적으로, 패밀리 I 모델들(Family I Models)로 지칭되는 제1패밀리는 IBM 퍼스널 컴퓨터 AT와, 다른 IBM 호환(IBM compatible) 기계에서 예를 찾아볼 수 있는 버스 구조(bus architecture)를 사용한다. 패밀리 II 모델들(Family II Models)로 지칭되는 제2패밀리는 IBM의 퍼스널 시스템/2 모델들 57부터 95에서 예를 찾아볼 수 있는 IBM의 마이크로 채널(MICRO CHANNEL) 버스 구조를 사용한다. 초기 패밀리 I 모델들은 전형적으로 시스템 프로세서로서 INTEL 8088 또는 8086 마이크로프로세서를 사용하였다. 후기의 소정 패밀리 I과 패밀리 II 모델들은 전형적으로 고속의 INTEL 80286, 80386과 80486 마이크로프로세서들을 사용하며 이들 마이크로-프로세서들은 저속의 INTEL 8086 마이크로프로세서를 에뮬레이트(emulate)하는 실모드(real mode)에서 작동이 가능하거나, 몇몇 모델들의 경우 어드레싱 범위(addressing range)를 1메가바이트로부터 4기가바이트로 확장하는 보호모드(protected mode)로 작동할 수 있다. 본질적으로, 상기 80286, 80386과 80486 프로세서들의 실모드 기능은 8086과 8088용으로 작성된 소프트웨어

어에 적합한 하드웨어 호환성을 제공한다.

IBM 퍼스널 컴퓨터와 같은 패밀리 I 모델들의 최초 퍼스널 컴퓨터 시스템으로부터 소프트웨어 호환성은 가장 중요하게 인식되었다. 이러한 목적을 달성하기 위하여, 펌웨어(firmware)라고도 알려진 시스템 상주 코드(System resident code)로 된 중간층(intermediate layer)이 하드웨어와 소프트웨어 사이에 설정되었다. 이러한 펌웨어는 사용자의 응용프로그램(application program)/운영체제(operation system)와 장치 사이에 운영 인터페이스(operational interface)를 제공함으로써, 사용자가 하드웨어 장치의 특징을 일일이 고려할 필요성을 제거하였다. 결국, 상기 코드는 새로운 하드웨어 장치가 추가될 수 있도록 허용함과 동시에 기존 응용프로그램이 하드웨어 특이성(hardware peculiarities)에 의해 영향받지 않도록 하는, 기본 입출력시스템(Basic Input/Output System(BIOS))으로 개발되었다. BIOS의 중요성은 그 즉시 자명한데, 그 이유는 BIOS의 존재로 인하여 장치구동기(device driver)가 특정장치의 하드웨어 특성에 종속적인 상태에서 벗어나 그 장치에 즉시 인터페이스할 수 있기 때문이다. BIOS는 시스템의 필수 부분이며 시스템 프로세서의 데이터 입출력동작을 제어하기 때문에, BIOS는 시스템 플래너상에 상주하며, 판독전용 기억장치(ROM) 내에 저장되어 사용자에게 제공되었다. 예를 들면, 초기 IBM 퍼스널 컴퓨터내의 BIOS는 플래너 기판상에 놓이는 ROM의 8K 바이트를 차지하였다.

새로운 모델의 퍼스널 컴퓨터 패밀리가 소개됨에 따라, BIOS는 새로운 하드웨어와 I/O 장치들을 포함하도록 갱신되고 확장되어야 했다. 예상했던바 대로, BIOS는 메모리 용량면에서 증가되기 시작했다. 예를들면, IBM 퍼스널 컴퓨터 AT의 등장과 더불어, BIOS는 32K 바이트의 ROM 을 필요로할 만큼 확장되었다.

오늘날, 새로운 기술의 개발과 더불어, 패밀리 II 모델의 퍼스널 컴퓨터 시스템들은 훨씬 더 정교해졌으며 소비자에게 더욱 빈번히 이용되도록 제작되고 있다. 기술은 급속도로 변하고 새로운 I/O 장치들의 퍼스널 컴퓨터 시스템에 추가됨에 따라, BIOS의 수정은 퍼스널 컴퓨터의 개발주기에 매우 중대한 문제가 되었다..

예를들면, 마이크로 채널 구조(Micro Channel Architecture)를 갖는 IBM 퍼스널 시스템/2(IBM PS/2)의 등장과 더불어, 진보된 BIOS(advanced BIOS) 또는 AB BIOS로 알려진 매우 새로운 BIOS가 개발되었다. 그러나, 소프트웨어 호환성을 유지하기 위하여, 패밀리 I 모델들의 BIOS는 패밀리 II 모델들내에 포함되어야만 하였다. 패밀리 I BIOS는 따라서 호환 BIOS(Compatibility BIOS) 또는 CB BIOS로 알려져 왔다. 그러나, IBM 퍼스널 컴퓨터 AT와 관련하여 전술한 바와같이, 단지 32K 바이트의 ROM이 플래너 보드상에 장치되었다. 다행스럽게도, 시스템은 96K 바이트의 ROM으로 확장될 수 있으나, 불행하게도, 시스템 제약 때문에, 96K 바이트의 ROM이 BIOS에 대해 사용할 수 있는 최대용량으로 밝혀졌다. 다행히, AB BIOS의 부가에도 불구하고, AB BIOS와 CB BIOS는 여전히 96K의 ROM에 저장될 수 있었다. 그러나, 96K ROM 영역중 확장에 이용될 수 있도록 남아 있는 부분은 적다. 장래 I/O 장치들의 부가에 의해 CB BIOS와 AB BIOS는 ROM 용량을 고갈시킬 것으로 믿어진다. 따라서, 새로운 I/O 기술은 CB BIOS와 AB BIOS내에 용이하게 통합될 수 없을 것이다.

이러한 문제들과 패밀리 II BIOS를 개발 주기상 가능한한 늦게 수정하고자 하는 요망에 의해 ROM으로부터 BIOS의 부분적인 오프로드(offload)가 필요하게 되었다. 이러한 제거는 BIOS의 부분을 고정디스크와 같은 대용량 저장장치상에, 바람직하게는 시스템 구획(system partition)으로 알려진 디스크의 한정된 부분내에 저장함으로써 달성한다. 시스템 구획은 또한 시스템 참조디스켓(system reference diskette)의 이미지(image)를 저장하는데, 이미지는 시스템 구성(system configuration)을 설정하는데 사용되는 소정의 유틸리티 프로그램(utility program) 또는 이와 유사한 프로그램을 포함한다. 디스크는 기록 및 판독능력을 제공하기 때문에, 디스크상의 실제적인 BIOS코드의 수정이 가능했다. 디스크는 비록 BIOS코드를 빠르고 효과적으로 저장할 수 있는 방법을 제공하나, BIOS코드가 훼손될 가능성을 크게 증가시켰다. BIOS는 운영체제(operating system)의 필수 구성부분이기 때문에, 잘못된 BIOS는 파괴적인 결과를 유발할 수 있으며 많은 경우에는 시스템의 완전한 고장 및 비구동의 원인이 될 수도 있다. 따라서, 고정디스크상에 BIOS코드가 허가없이 수정되는 것을 방지하기 위한 수단이 매우 요망되는 것을 분명하다. 이것은 1989년 8월 25일 출원된 미국 특허출원 제C/396,320호로서, 1991년 6월 4일 등록된 미국 특허 제5,022,077호의 요지였다. 이 특허는, 본 명세서에 개시된 본 발명의 이해에 유용한 부가적 정보로서, 관심있는 사람들에게 참조될 수 있으며, 본 명세서에 개시된 본 발명을 완전히 이해하는데 필요한 정도로 본 명세서에서 참고문헌으로 인용된다.

IBM의 PS/2의 등장과 더불어 마이크로 채널 시스템들은 I/O 어댑터 카드와 플래너에서 스위치들과 정퍼들을 제거하였다. 상기 마이크로채널 아키텍처는 스위치 및 플래너를 제거하는 대신에 프로그램 가능한 레지스터를 제공하였다. 이러한 프

로그 가능 레지스터 또는 프로그램 가능 옵션 선택(Programmable option select)(POS) 레지스터를 구성하기 위해 유틸리티가 요구되었다. 상술한 유틸리티 그리고 '시스템 진단(diagnostics)과 더불어 시스템 가용성 특징(usability characteristics)을 개량하기 위한 다른 유틸리티들이 각 시스템에 시스템 참조 디스켓상에서 제공되었다.

최초 사용 전에, 각 마이크로 채널 시스템은 POS 레지스터들이 초기화되도록 요구한다. 예를 들어, 상기 시스템이 새로운 I/O 카드를 채용한 채 또는 I/O 카드용 슬롯을 변경한 채 부트(boot)되면, 구성(configuration) 에러가 발생되고 시스템 부트업(boot up) 과정이 중단된다. 그러면 사용자는 그 후 시스템 참조 디스켓을 로드(load)하고 F1 키를 누르도록 촉구된다. 그러면 세트 구성 유틸리티(A Set Configuration Utility)가 시스템을 구성하기 위하여 시스템 참조 디스켓으로 부트될 수 있다. 상기 세트 구성 유틸리티는 사용자가 요구된 동작을 하도록 촉구한다. 적절한 디스크립터 파일(descriptor files)이 시스템 참조 디스켓에 적재(load)되면, 상기 세트 구성 유틸리티는 비휘발성 저장장치 내에 정확한 POS 또는 구성 데이터를 형성 한다. 상기 디스크립터 파일은 상기 카드를 상기 시스템에 인터페이스(interface)하는 구성 정보를 보유한다.

근년의 세계적인 퍼스널 컴퓨터의 경이적 증가와 사용에 의해, 더 많은 데이터 또는 정보들이 수집되어 이러한 시스템 내에 보유 또는 저장되고 있다. 이들 데이터의 많은 부분은 속성상 매우 민감하다. 따라서, 데이터가 잘못 취급되면, 데이터가 사용자 각각을 당혹시키거나, 사업자가 경쟁력을 상실하거나, 또는 민감한 데이터가 침묵의 대가를 지불하도록 강요하는 수단으로 이용되거나 또는 각 사용자에게 대한 물리적 피해를 유발할 수 있다. 더 많은 사용자가 데이터의 민감한 성질과 가치를 깨닫게 됨에 따라, 데이터의 이러한 오용을 방지하는 것이 더욱 요망되었다. 저장된 데이터 자신과 저장된 데이터에 관련된 사용자들을 보호하기 위하여, 사용자들은 그들이 구입하는 퍼스널 컴퓨터 내에 보안 및 무결성(integrity) 기능이 병합을 요구하고 있다.

사용자만이 수집되어 저장된 데이터의 민감성을 인식하고 있는 것은 아니다. 정부들 역시 민감한 데이터의 보호를 강제하는 법률들을 제정하고 있다. 이러한 정부의 예는 미합중국이다. 미합중국은 상황의 중대성을 인식하고 대책을 제거하였다. 미합중국 연방정부는 보안수준(security level)과 보안수준들을 충족시키는데 필요한 필요 조건들을 규정하여 왔고, 인증관청(certification agency)을 설치하여 퍼스널 컴퓨터 제조업자들에게 제품을 제출토록 하여 제출한 제품이 제조업자들이 주장한 보안수준을 충족하고 있는지의 여부를 검사하고 있다. 연방정부 요건들의 근원은 일반적으로 오렌지책(Orange book)으로 인용되는, 국방성의 신뢰 컴퓨터 시스템 평가 기준(Trusted Computer System Evaluation Criteria), DOD 5200. 28 STD, 12/85 이다. 정부는 정부와 관련된 모든 데이터가 1992년 1월 1일까지 최소한의 보안수준인 C-2로 처리되어 퍼스널 컴퓨터에 저장되어야 한다고 입법하였다. 컴퓨터 시스템 하드웨어에 대한 본질적인 요건들은 보증부분(Assurance section), 요건 6 : 신뢰할 만한 메카니즘은 무단조작(tampering) 및/또는 권한 없는 변경에 대해 끊임없이 보호되어야 하며....에 수록되어 있다.

상기한 사항에 미루어, 본 발명은 보안 시스템이 되는 능력을 가진 퍼스널 컴퓨터가 비보안 기계(unsecured machine)에 대한 공격에 의해 보안 시스템이 되는 것을 방지한다. 이러한 공격이 성공한다면, 시스템 소유자(system owner)는, 시스템이 소망하는 바에 의해 비보안 상태로 되었을 때 적절히 시스템에 저장된 데이터도 접근할 수 없게 될 것이다.

퍼스널 컴퓨터 시스템에 보안기능을 유지하려는 접근법은 시스템에 부가적인 구성 요소들을 사용할 수 있다. 본 발명은, 이러한 부가적인 구성 요소들을 제공하고, 후술하는 바와같이 부가적 보안 구성요소들을 BIOS 조직에 적응시킨다.

퍼스널 컴퓨터 내에 제공된 보안 설비(security provisions)를 사용하여 바람직한 효과를 얻을 수 있는 환경중 하나는, 다수의 시스템이 상호 연결되고 또한 중앙 파일 서버 시스템(central file server system)에도 연결될 수 있는 네트워크(network)이다. 이러한 네트워크에 있어서는, 비보안 얼터네이트(alternate)로 대체하고 그 비보안 시스템을 통하여 공격하기 위해 네트워크를 오픈(open)하는 행위에 대비하여 네트워크가 모든 소정의 특정한 시스템을 식별할 수 있도록 네트워크 보안을 유지하는 것이 중요하다.

본 발명의 몇가지 목적들이 기술되었으며 다른 목적은 첨부된 도면과 관련하여 설명될 것이다.

본 발명의 바람직한 실시예가 도시되어 있는 첨부 도면을 참고하여 본 발명을 이하에서 설명한다. 그러나, 본 발명의 기술분야에 통상의 지식을 가진 자는 본 명세서에 기재된 본 발명을 변형하여 본 발명의 바람직한 결과를 얻을 수 있음을

발명 설명의 개시부터 이해하여야 한다. 따라서, 다음의 설명은 본 발명의 기술 분야에서 통상의 지식을 가진 자에 대한 광범위하고 교시적인 내용으로서 이해되어야 하며, 본 발명을 제한하는 것으로 이해 되어서는 안된다.

본 명세서에서 사용되는 소정의 정의된 용어는 다음과 같다.

신뢰 계산 베이스(TRUSTED COMPUTING BASE)(TCB) : 하드웨어, 펌웨어와 소프트웨어를 포함하는 컴퓨터 시스템내 전체 보호 메카니즘(protection mechanisms)들. 이들의 조합이 보안정책(security policy)을 시행하는 역할을 담당한다. TCB는 하나 또는 그 이상의 구성요소로 이루어지고 이들 구성요소가 제품 또는 시스템에 대하여 통합된 보안 정책을 시행한다. 보안 정책을 정확히 시행하기 위한 TCB의 능력은 전적으로 TCB내의 메카니즘과 보안 정책과 관련한 파라미터(예를들어, 사용자의 완전 무결함(clearance))의 시스템 관리 요원(system administrative personnel)에 의한 정확한 입력에 달려있다.

신뢰 소프트웨어(TRUSTED SOFTWARE) : 신뢰 계산 베이스의 소프트웨어 부분.

신뢰 프로그램(TRUSTED PROGRAM) : 신뢰 소프트웨어에 포함된 프로그램.

개방 프로그램(OPEN PROGRAM) : 신뢰 프로그램을 제외한, 신뢰 계산 베이스상에서 동작 가능한 프로그램.

참조 모니터 개념(REFERENCE MONITOR CONCEPT) : 주체(Subjects)에 의한 대상(objects)으로의 모든 액세스를 중재하는 추상적 기계(abstract machine)를 참조하는 액세스 제어 개념.

보안 커널(SEcurity KERNEL) : 참조 모니터 개념을 구현하는 신뢰 계산 베이스의 하드웨어, 펌웨어 및 소프트웨어 요소들. 보안 커널은 모든 액세스들을 중재해야 하며, 수정(modification)으로부터 보호되어야 하고, 정확하다는 것이 입증될 수 있어야 한다.

신뢰 컴퓨터 시스템(TRUSTED COMPUTER SYSTEM) : 충분한 하드웨어 및 소프트웨어의 무결성(integrity)수단을 채용하여 일정 범위의 민감하거나 비밀스런 정보를 동시에 처리하도록 허용하는 시스템.

시스템 소유자(SYSTEM OWNER) : 시스템 소유자는 초기에 시스템을 보안 모드로 구성하고 지정해 주는 책임이 있는 사용자이다. 시스템 소유자는 초기때와 갱신이 요구될 때마다 구성을 제어할 것이다. 이러한 소유자는 특권 액세스 암호(Privileged Access Password)를 관리할 것이며, 이 암호의 무결성을 유지하는 책임이 있다. 시스템 소유자는 또한 무단 조작 확증 덮개 잠금 키(tamper evident cover keylock key)의 물리적 보안을 유지시켜야 한다. 시스템 소유자는 모든 시스템상의 보안 등재(log)들을 유지시켜야 한다. 시스템 소유자는 또한 시도되었던 모든 보안 침해(security breaches)를 기록해야 할 것이다. 시스템 소유자는 하나이상의 시스템을 소유할 수 있다. 시스템 소유자는 인가(authorized)된 사용자로 간주되며, 또한 정규 사용자로도 될 수 있다.

보안 모드(SECURE MODE) : 시스템 사용자가 보안 및 무결성요소들에 의해 제공되는 보안 보호(security protection)를 강구하기 위하여 특권 액세스 암호를 퍼스널 컴퓨터 시스템에 성공적으로 설치한 때.

인가된 사용자(AUTHORIZED USER) : 특권 액세스 암호의 사용을 인가받은 모든 사용자. 이러한 사용자는 시스템 소유자일 수도 있고 또는 시스템 소유자가 아닐 수도 있다. 이러한 사용자는 또한 특정 시스템 또는 일련의 시스템의 키를 보유할 수 있다. 이러한 사용자가 보안 침해로부터 시스템을 복귀시키는데 관련된다면, 이들은 그 보안 침해를 시스템 소유자에게 보고할 책임이 있다. 인가된 사용자는 또한 정규 사용자로도 될 수 있다.

정규 사용자(NORMAL USER) : 시스템 설비를 이용하도록 인가된 모든 사용자. 시스템 구성을 변경하거나, 문제를 해결하기 위하여, 이러한 사용자는 시스템 소유자 또는 인가된 사용자의 협조를 필요로 한다. 정규 사용자는 그들이 인가된 사용자 또는 시스템 소유자의 범주에 속하지 않는 한 특권 액세스 암호나 무단조작 확증 커버 잠금 키를 소유하지 않는다.

비인가 사용자(UNAUTHORIZED USER) : 시스템 소유자, 인가된 사용자 또는 정당 사용자가 아닌자. 보안된 퍼스널 컴퓨터가 비인가 사용자에 의해 사용된 경우는 모든(단, 전원공급조작(power on)의 실패의 경우 제외)보안 침해로 간주되며, 이러

한 침해를 나타내는 감사 추적(audit trail)이 반드시 존재하여야 한다.

EEPROM : 전기적 소거 및 프로그램 가능한 판독전용 메모리. 이러한 메모리 기술은 데이터를 비휘발성으로 저장하며 하드웨어 로직의 제어하에 데이터를 변경시킬 수 있다. 저장된 내용은 전원공급이 중단되어도 소실되지 않는다. 저장내용은 모듈상의 적절한 제어신호들이 사전 규정된 순서로 활성화될 때만 변경될 수 있다.

암호 디스크립션(PASSWORD DESCRIPTION) : 시스템은 2개의 암호 예컨데, 1. 특권 액세스 암호(PAP) 및 2. 파워 온 암호(Power On Password)(POP)로 보호될 수 있다. 이러한 암호들은 서로 독립적으로 사용되도록 의도된다. PAP은 초기 프로그램 적재(Initial Program Load)(IPL)장치 부트 리스트(device boot list), 암호 유틸리티로의 액세스 및 시스템 참조 디스켓 또는 시스템 구획으로의 액세스를 보호함으로써, 시스템 소유자를 보호하도록 설계되어 있다. PAP가 설치(install)되지 않았거나 파워 온 시퀀스 동안 초기에 PAP가 정확하게 인가되어야만, 시스템 구획은 POST에러에 응답하여 부트될 것이다. 디스켓으로부터의 초기 BIOS적재(Initial BIOS Load) (IBL)는 시스템 참조 디스켓을 부팅하는 것과 동일한 방식으로 보안될 것이다. PAP의존재는 POP를 사용하는 정규 사용자에게는 명백(transparent)할 것이다. PAP는 시스템 참조 디스켓상의 또는 시스템 구획내의 유틸리티에 의해 설치되거나 변경되거나 소거될 것이다. PAP는 정확하게 세트되고 인가될 때, POP을 무효화함으로써 사용자가 전체 시스템에 액세스할 수 있게 한다. 현재의 모든 P/2 시스템에서 작용하는 POP는 DASD상의 운영체제 또는 시스템 설비에 대한 허가되지 않은 액세스를 방지하는데 사용된다.

첨부된 도면을 참조하면, 본 발명을 구체화하는 마이크로 컴퓨터(10)가 도시되어 있다(제1도). 상술한 바와같이, 컴퓨터(10)는 모니터(11), 키보드(12) 및 프린터 또는 플로터(14)를 구비할 수 있다. 컴퓨터(10)는 덮개(15)를 구비하며, 이 덮개는 제2도에 도시된 바와같이, 샤시(chassis)(19)와 협력하여 디지털 데이터를 처리 및 저장하도록 전기적으로 구동되는 데이터 처리 및 저장 구성요소를 수용하기 위하여 감싸지고 보호되는 용적체를 형성한다. 제2도에 도시된 형상에서, 컴퓨터(10)는 또한 선택적 I/O케이블 연결 덮개(16)를 가지며, 이 연결 덮개(16)는 I/O케이블들과 컴퓨터 시스템과의 연결지점을 넘어 연장되어 그 연결지점을 보호한다. 적어도 소정의 이러한 시스템 구성요소들은 다층 플래너(20)(본 명세서에서는 마더 보드 또는 시스템 보드라고도 기술된다)에 장착되며, 이 다층 플래너(20)는 샤시(19)상에 장착되며 전술한 바와같은 구성 요소들과 플로피 디스크 구동장치, 다양한 형태의 직접 액세스 저장장치(direct access storage devices) 및 부속 카드 또는 보드등과 같은 다른 연관된 요소들을 포함하는 컴퓨터(10)의 구성요소들을 전기적으로 상호 연결하는 수단을 제공한다.

샤시(19)는 베이스와 후면 패널(panel)(제2도 참조, 이것은 케이블 연결덮개(16)에 의해 외부적으로 덮혀질 수 있다)을 가지며, 자기 또는 광학 디스크용 디스크 구동장치, 또는 테이프 백업 구동장치(tape backup drive)등의 저장장치를 수용하는 최소한 하나의 개방된 만(bay)형상의 공간을 형성한다. 도시된 형태에서, 상부 공간(22)은 (3.5인치 구동장치로 알려진 것과 같은)제1사이즈의 주변 구동장치(peripheral device)를 수용하는데 적합하다. 상부 공간(22)에는, 일반적으로 알려진 바와같이 삽입되는 디스켓을 수용하고 이 디스켓을 이용하여 데이터를 입력, 저장 및 전달할 수 있는 제거가능한 매체 직접 액세스 저장장치(removable media direct access storage device), 즉 플로피 디스크 구동장치가 제공될 수 있다.

상기 구조를 본 발명에 결부시키기 전에, 퍼스널 컴퓨터 시스템(10)의 일반적 작동의 개요를 재검토할 필요가 있다. 제3도를 참조하면, 플래너(20)상에 장착되는 구성요소들과, I/O슬롯들 및 퍼스널 컴퓨터 다른 하드웨어와 플래너와 연결을 포함하는 (본 발명에 따른)시스템(10)과 같은 컴퓨터 시스템의 각종 구성요소들을 나타내는 퍼스널 컴퓨터 시스템의 블럭도가 도시되어 있다. 플래너에는 시스템 프로세서(32)가 연결된다. 어떠한 적절한 마이크로 프로세서라도 CPU(32)로서 사용될 수 있으나, INTEL사에서 판매하는 80386이 하나의 적합한 마이크로프로세서이다. CPU(32)는, 고속의 국부버스(local bus)에 의해, 버스 인터페이스 제어 유닛(35)와, 본 명세서에서 싱글 인라인 메모리 모듈(Single Inline Memory Modules)(SIMM)로서 도시된 휘발성 랜덤 액세스메모리(RAM)(36)와, CPU(32)와의 기본 I/O출력 작동(basic input/output operations)을 위한 명령이 저장되는 BIOS ROM(38)에 연결된다. BIOS ROM(38)은 I/O장치들과 마이크로프로세서(32)의 운영체제를 인터페이스하는데 사용되는 BIOS를 포함한다. BIOS ROM(38)에 저장된 명령들은 BIOS의 실행 시간을 단축시키기 위하여 RAM(36)내로 복사될 수 있다. 이 시스템은 또한, 통상적인 것으로서, 시스템 구성에 필요한 데이터를 입력하고 저장하는 배터리 백업 비휘발성 메모리(통상적으로 CMOS RAM)를 갖는 회로 성분과 실시간 클럭(real time clock)(RTC)(68)(제3도와 제4도)을 구비한다.

이하에서 본 발명은 특히 제3도의 시스템 블록도를 참조하여 설명되지만, 다음 설명의 개시에서부터 본 발명에 따른 장치 및 방법이 플래너 보드의 다른 하드웨어 구성과 함께 사용될 수도 있음이 의도된다는 것을 이해하여야 한다. 예를들면, 시스템 프로세서는 INTEL 80286 또는 80486 마이크로프로세서 일 수도 있다.

제3도를 참조하면, (데이터, 어드레스와 제어 성분을 구비하는)CPU국부버스(34)는 또한 마이크로프로세서(32)를 마스크 프로세서(math coprocessor : MCP)(39)와 소형 컴퓨터 시스템 인터페이스(Small Computer System Interface)(SCSI)제어기(40)에 연결시켜 준다. 컴퓨터 설계 및 운영 기술분야에서 통상의 지식을 가진자에게 알려진 바와같이, SCSI 제어기(40)는 판독전용 메모리(ROM)(41), RAM(42) 및 도면 우측에 도시된 /O연결에 의해 쉽게 연결되는 각종 형태의 적합한 내부 또는 외부장치에 연결되거나 연결될 수 있다. SCSI 제어기(40)는 (하드(hard)와 플로피 디스크 구동장치로도 알려져 있는)고정 또는 제거가능한 전자기 매체 저장장치, 전-광 테이프 및 다른 저장장치와 같은 저장 메모리장치(storage memory devices)를 제어하는 저장장치 제어기(storage controller)로서 기능을 한다.

버스 인터페이스 제어기(BIC)(35)는 CPU국부버스(34)와 /O버스(44)를 연결한다. 버스(44)에 의하여, BIC(35)는 /O장치 또는 메모리(도시되지 않음)에 더 연결될 수도 있는 마이크로채널 어댑터 카드(MICRO CHANNEL adapter card)를 수용하는 다수의 I/O슬롯들을 가지는 마이크로 채널 버스(MICRO CHANNEL bus)와 같은 선택적 기능 버스(optional feature bus)에 연결된다. I/O버스(44)는 어드레스, 데이터 및 제어 성분을 포함한다.

I/O버스(44)를 따라서 그래픽 정보 저장용 비디오 RAM(VRAM)(48) 및 영상 정보 저장용 비디오 RAM(49)과 연관된 비디오 신호 프로세서(video signal processor : VSP)(46)와 같은 다양한 /O성분들이 결합된다. 프로세서(46)와 교환된 비디오 신호들은 디지털 아날로그 변환기(DAC)(50)를 통하여 모니터 또는 다른 디스플레이 장치에 전달될 수 있다. 비디오 기/기 재생기, 카메라등의 형태를 취할 수 있는, 본 명세서에서 자연 영상 입출력장치(natural image input/output)로 지칭되는 장치와 VSP(46)를 직접 연결하는 설비가 또한 형성되어 있다. /O버스(44)는 또한 디지털 신호 프로세서(Digital Signal Processor : DSP)(51)에 연결되며, 이 DSP(51)는 DSP(51)에 의한 신호 처리용 소프트웨어 명령들과 이러한 신호 처리에 수반되는 데이터를 저장하는데 이용할 수 있는 명령어 RAM(instruction RAM)과 데이터 RAM(data RAM)(54)을 구비한다. DSP(51)는 오디오 제어기(55)가 제공됨으로써 오디오 입력 및 출력을 처리하며, 아날로그 인터페이스 제어기(analog interface controller) (AIC)(56)가 제공됨으로써 다른 신호들을 처리할 수 있다. 마지막으로, /O버스(44)는 EEPROM(Electrical Erasable Programmable Read Only Memory)(59)과 연결된 입출력 제어기(58)에 결합되며, 입력 및 출력은 입출력 제어기(58) 및 직렬포트에 의해 플로피 디스크 구동장치, 프린터 또는 플로터(14), 키보드(12), 마우스 또는 포인팅 장치(pointing device)(도시되지 않음)를 포함하는 통상의 주변장치들과 교환된다. EEPROM은 이하에서 기술되는 보안 설비에서 한 역할을 담당한다.

이제까지 서술된 시스템(10)은 보안설비가 소망될 뿐더러 요구되는 응용에서 사용될 수 있을 뿐만 아니라 보안 설비가 필요치 않고 실제로 소망되지도 않는 응용에서 사용될 수 있음이 이해될 것이다. 임의의 주어진 시스템이 이러한 환경중 어느 하나 또는 양자모두에게 사용될 수 있음을 안다면, 시스템 제작자는 반드시 상기환경중 어느 하나에서라도 사용할 수 있는 시스템을 준비해야 한다. 본 명세서에 서술된 본 발명의 초점은 상기한 두가지 환경에서 적응할 수 있는 시스템 표현이다.

하나의 특정한 예는 비보안(non-secured)시스템은 바람직하지 않게 보안 시스템이 되지 못하도록 방지 되어야 한다는 것이다. 그러한 전환이 발생했을 때의 하나의 결과로는 비보안 시스템에 저장된 데이터는 시스템이 암암리에 보안 시스템으로 전환되었을 때, 이용불가능하게 된다는 것이다. 이러한 경우는 보안설비를 갖추었으며 시스템 소유자가 그 보안 설비를 작동시키지 않기로 정한 경우에 발생할 수 있다.

본 명세서에서 기술된 바와같이 퍼스널 컴퓨터 시스템에 보안을 유지하는 소정 목적들을 달성하는데 있어서, 퍼스널 컴퓨터 시스템(10)은 시스템 봉합체(system enclosure)내에 장착되어 활성상태와 비활성 상태를 선택하며 활성 상태일 때 특권 액세스 암호(PAP)를 수신하고 저장하기 위한 소거 가능한 메모리 소자를 가지고 있다. 소거 가능한 메모리 소자로서 전술한 전기적으로 소거 및 프로그램 가능한 판독 전용 메모리 장치, 즉 EEPROM(59)(제3도)의 한 필드(field) 또는 부분이 바람직하다. 시스템은 또한 봉합체내에 장착되며 상기 소거 가능한 메모리 소자(59)에 작동적으로 연결되어 그 메모리 소장의 상기 필드 또는 부분을 활성 및 비활성 상태로 세트하는 선택스위치(option switch) 즉 보안스위치(security

switch)를 가지고 있다. 선택스위치(또한 보안스위치라고도 지칭된다)는, 예컨대, 상기 시스템 플래너(20)상에 장착되는 점퍼(jumper)일 수 있으며, 플래너에 접근(access)하는 사용자에게 의해 수동적으로 2개의 상이한 상태로 설정 가능하다. 그 중 한 상태(본 명세서에서 기록 가능 또는 비잠금 상태(write enable or unlocked state)라고도 언급된다)에서, EEPROM(59)은 활성상태로 세트되고 PAP를 저장한다. 기록 가능 상태에서, PAP는 EEPROM에 기록되거나, 변경되거나 소거될 수 있다. 이와는 다른 비활성상태(본 명세서에서 기록불능 또는 잠금 상태(write disabled or locked state)라고도 언급된다)에서는, EEPROM의 PAP 저장능력은 비활성 상태로 세트된다.

본 명세서에 기술된 본 발명의 소정기능에 따라, EEPROM은 또한 상기 시스템(10)이 보안 네트워크(secure network)로 연결되고 본 명세서에 기술된 보안 기능이 활성상태일 때, 네트워크 서버(network server)가 접근할 수 있고 제작자에 의해 설치된 시스템 유일 식별자(system unique identifier)를 또한 포함한다.

상술한 바와같이, 시스템(10)은 또한 (68)로 표시된 제2성분을 구비하며, 제2성분은 소거 가능한 메모리능력, 즉 배터리 지원 비휘발성 CMOS PAM과, 이와 관련된 실시간 클럭(RTC)을 구비한다. CMOS RAM은, 본 발명에 따라, 상기 시스템(10)의 전원공급시 PAP의 성공적인 입력에 관한 데이터를 포함하는 시스템 구성을 나타내는 데이터를 저장한다. 적어도 하나의 무단조작 검출 스위치가 제공되는데, 이 검출 스위치는 봉합체내에 장착되고 CMOS RAM에 작동적으로 연결되어 봉합체의 비인가된 개방시 무단조작 검출 스위치의 스위칭에 응답하여 봉합체의 개방을 검출하고 그 메모리 소자내에 저장된 소정 데이터를 클리어 또는 세트시킨다.

전술한 보안 및 무결성 기능은 앞서 제안된 퍼스널 컴퓨터 보안기능 즉, 파워 온 암호(Power On Password: POP)와는 무관하게 작용한다. 이러한 부가적 보안 및 무결성 기능은 오렌지 북(Orange Book)과 같은 적용 가능한 규칙들하에서 시스템 인증을 운영하기 위한 보안 플랫폼(secure platform)을 제공한다. 시스템을 보안 모드(secure mode)로 설정하기 위해 하나의 부가적인 패스워드가 필요하다. 새로운 패스워드는 본 명세서에서 특권 액세스 암호(Privileged Access Password: PAP)로 언급된다. 기존의 퍼스널 컴퓨터 시스템과의 호환성을 유지하기 위해서, POP도 역시 유지된다.

암호 보안은 다음과 같은 시스템 하드웨어 기능들에 의해 구현된다 : EEPROM, 보안스위치 무단조작확증 덮개 스위치(tamper evident cover switch), 펌웨어, PO ST 및 시스템 소프트웨어 암호 유틸리티(system software password unility). PAP가 설치되면, 상기 시스템은 보안 모드로 된다. PAP는 EEPROM내에 저장(save)된다. PAP의 백업 카피(backup copy) 역시 EEPROM에서 유지된다. 이것은 PAP의 설치, 변경, 또는 제거 동안에 전원 고장이 발생했을때, PAP의 우발적인 손실을 막는다. POP와, (설치된 경우)PAP의 유효성(validity)을 나타내는 최소한의 소정 비트(bit)가 CMOS RTC에 저장된다. CMOS RTC 및 EEPROM에 보유된 데이터의 변경은 상호독립이다.

제4도는 통상의 전원 제어장치, 즉 온/오프스위치(61), 통상의 전원공급장치(62), 본체덮개(15) 및 케이블연결덮개(16)와 같은 봉합체덮개의 개방 또는 제거에 따라 전도상태(conductive state)가 변하는 스위치들과 키록 스위치(64)의 관계를 도시한다. 봉합체 덮개의 개방 또는 제거시 상태가 변하는 스위치들은, 예시된 본 발명의 형태에서, 본체덮개(15)의 제거에 응답하는 스위치(65)(제4, 5와 6도)와 케이블연결덮개(16)의 제거에 응답하는 스위치(66)(제4, 5와 7도)의 두가지이다. 각 스위치는 정상시 개방 구성요소(65a) 및 (66a)과 정상시 폐쇄 구성요소(65b) 및 (66b)의 두가지 구성요소를 가지고 있다. 제2스위치(66)는 케이블연결덮개(16)와 마찬가지로 선택적이다. 그러나, 본 명세서에 개시된 본 발명을 주의깊게 고려하면 명백해지는 바와같이, 선택적인 덮개와 스위치의 존재는 시스템에 대한 더욱 완벽한 안전제어를 담보한다.

덮개스위치(65) 및 (66)의 정상시 개방 점점 세트들은 주전원스위치(61)와 전원공급장치(62)에 직렬로 연결된다(제4도). 결과적으로, 덮개를 제거한 채로 시스템(10)을 파워 업하려고 시도하면, 점점 세트들(65a) 및 (66a)은 개방되어 시스템구동을 방지한다. 덮개가 제위치에 있는 경우, 점점 세트들은 폐쇄되어 정상적인 시스템 동작이 개시될 수 있다.

덮개스위치들(65) 및 (66)의 정상시 폐쇄 점점 세트들을 키록스위치(64)와 RTC 및 COMS메모리(68)에 직렬로 연결된다. 정상시 폐쇄 점점세트(65b) 및 (66b)는 덮개(15), (16)가 존재할 때에는 개방되며 이러한 덮개의 제거시에는 폐쇄될 것이다. 키록스위치(64)는 통상적으로 컴퓨터 시스템(10)에 제공되는 열쇠로 잠겨질 때 잠금 상태를 유지한다. 이러한 3개의 점점세트들은 RTC 및 CMOS 메모리부분을 여기(energizing)시키는 전류를 접지로 흐르게하는 교번(alternate)통로를 제공하며, 시스템이 잠금상태에서 덮개가 무단제거될 때, 여기화(energization)가 상실되어 메모리의 세크먼트를 (전부 1의 상태와

같은) 별도의 상태로 세트하는 효과를 가진다. 상기 메모리가 POST에 의해 체크되므로 별도의 상태로 상기 세그먼트를 세트하는 것은 구성 에러신호를 발생시켜 시스템 소유자에게 시스템 보안을 파괴하고자 하는(성공적이든 아니든)시도가 있었음을 경고한다. 메모리 세그먼트가 이렇게 별도의 상태로 세트되었을 때, 운영체제를 부팅하기 위해서는 사전 저장된 암호가 필요하다. 즉, 운영체제를 부팅하려면 본 명세서에서 기술된 것처럼 유효한 PAP의 입력이 필요하다.

키록스위치(64) 및 본체덮개스위치(65)는 바람직하게 전면의 카드 가이드부재(69)상에 장착되어(제2도 및 6도) 본체덮개(15)내에 제공된 자물쇠에 대하여 적절히 위치된다. 전면 카드 가이드부재는 덮개스위치(65)용 작동레버(70)가 수직의 전면 프레임 부재내의 개구를 통해 돌출하고 덮개(15)가 시스템 봉합체를 밀폐하도록 배치되어 있을 때 그 덮개(15)에 의해 작동되도록 컴퓨터 시스템 프레임내에 장착되어 있다.

케이블덮개스위치(66)는 바람직하게 시스템 프레임의 후면 패널에 장착되어 있고, 케이블덮개(16)상에 장착되어 있는 래치부재에 의해 작동되도록 배치되어 있고, 봉합체덮개(15)상에 있는 것과 유사한 수동으로 조작 가능한 키록의 제어하에 선회 가능하다. 선택케이블덮개(16)가 사용될 때(완벽한 시스템 보안이 요구 되거나 필요할 경우), 덮개의 후면 패널의 대한 래칭(latching) 또는 잠금(locking)은 래치부재로 하여금 정상시 개방 접점세트(66a)를 폐쇄하게 하며, 정상시 폐쇄 접점세트(66b)를 개방하게 한다.

본 발명에 따라서, 시스템(10)의 제작시 디폴트(default)상태는 파워-업시 시스템을 비보안 모드로 설정한다. 시스템이 보안시스템이 되게 하기위해, 시스템 소유자는 반드시 잠긴 덮개를 개방하여 시스템 플래너(20)상에 위치한 보안스위치의 상태를 의도적으로 변경시켜 상기 시스템을 보안시스템이 되게 하는 보안암호를 활성화시킨다. 그러므로 이제까지 서술된 보안기능의 존재로 인하여, 시스템 소유자 또는 다른 인가된 사용자도 모른 채 초기의 비보안시스템이 보안시스템으로 되는 것이 방지된다.

본 명세서에서 간단히 언급된 바와같이, 본 발명에는 부가적인 보안 구성요소들의 사용을 위한 대책이 제공된다. 보다 특정하게는, 다수의 제작들은 I/O 선택버스(44)를 경유하여 시스템에 연결된 카드(45)의 하나처럼 설치될 수 있는 선택 카드를 제공한다. 소정의 이러한 상업적으로 유효한 선택 카드가 사인인식 펜(signature recognition pen), 자기 스트라이프 카드(magnetic stripe card), 또는 토큰(token)을 포함한 ROM의 형태를 띌수 있는 암호화 키(encryption key)에 연결된다. 이러한 선택 카드가 보안상태로 설정된 시스템(10)과 같은 시스템에 부가되면 부가적인 보호수준이 제공될 수 있다. 또한, 이렇게 부가되었을때, 시스템 사용자만이 DASD시스템의 시스템 구획내에 보유된 참조디스켓의 이미지에 저장된 세트구성 유틸리티 프로그램(Set Configuration Utility Program)과 선택 카드로 접근할 수 있는 유일한 권한을 가진 사람이 된다.

본 발명은 또한 시스템 유일 식별자(system unique identifier)가 EEPROM (59)에 저장되도록 의도한다. EEPROM에 저장된 식별은, 시스템(10)이 연결된 네트워크 서버 또는 그것과 유사한 것에서 진행되는 소프트웨어로 접근할 수 있다. 그러므로 네트워크는 네트워크내의 특정 위치에 자리잡은 시스템이 조정된 접근이 허용된 보안시스템이며 또한 그러한 상태를 지속적으로 유지하는지 여부를 검증할 수 있다. EEPROM에 저장된 상기 식별은, EEPROM이 판독전용 장치이고, 메모리에 저장된 상기 식별에 어떤 변경을 가하려면 특별한 하드웨어를 필요로 한다는 사실에 의해 보호된다.

도면 및 본 명세서에서 본 발명의 바람직한 실시태양을 설명하였으며, 비록 특정의 용어가 사용되었어도, 그 설명은 일반적이고 개설적인 개념으로 그러한 용어를 사용한 것이며 본 발명을 국한시키려는 목적으로 사용한 것은 아니다.

(5) 청구항 범위

청구항 1. 데이터를 수신(receiving) 및 보유(retaining)하고, 시스템내에 보유된 데이터를 비인가된 액세스에 대하여 보안(secure)할 수 있는 퍼스널 컴퓨터 시스템에 있어서 : 통상 폐쇄된 봉합체(enclosure)와; 상기 봉합체를 안전하게 잠긴 상태(securely locked position)로 통상 유지하기 위한 것으로, 키(key)를 소지한 자와의 상기 봉합체내부에 대한 접근(access)을 부정하는 봉합체 자물쇠와; 상기 봉합체내에 장착되고 선택적으로 활성 상태 및 비활성상태로 작동하는 소거가능한 메모리소자와; 상기 봉합체내에 장착되고, 상기 봉합체내에서만 접근가능하며 상기 소거가능한 메모리소자

에 자동적으로 연결되어 상기 소거가능한 메모리소자를 활성 및 비활성 상태로 세트하는 선택스위치(option switch)와; 상기 봉합체내에 장착되고 상기 소거가능한 메모리소자에 작동적으로 연결되어, 상기 메모리소자의 활성 상태와 비활성 상태를 구별함으로써 상기 시스템내에 저장된 최소한 특정 수준(at least certain levels)의 데이터에 액세스하는 것을 제어하는 시스템 프로세서를 포함하는 퍼스널 컴퓨터 시스템.

청구항 2. 제1항에 있어서, 상기 선택스위치는 상기 메모리소자의 활성 상태와 비활성 상태를 각기 선택함으로써 조작자(operator)가 상기 시스템의 보안작동(secured operation)과 비보안 작동(unsecured operation)을 선택 할 수 있게 작동하는 퍼스널 컴퓨터 시스템.

청구항 3. 제2항에 있어서, 상기 선택스위치는 수동으로 조작 가능하며 상기 봉합체내에 배치되어 상기 봉합체가 개방된 후에만 수동으로 액세스 가능한 퍼스널 컴퓨터 시스템.

청구항 4. 제1항에 있어서, 상기 소거 가능한 메모리소자는 전기적으로 소거 및 프로그램 가능한 판독전용 메모리장치(electrically erasable programmable read only memory device)이고, 상기 전기적으로 소거 및 프로그램 가능한 판독 전용 메모리장치는 상기 퍼스널 컴퓨터 시스템이 연결된 네트워크 서버(network server)에서 실행(running)되는 소프트웨어를 인에이블(enabling)시키는 시스템 유일 식별자(system unique identifier)를 포함하되, 상기 소프트웨어는 상기 네트워크내의 특정 장소(particular location)에 위치한 시스템이 조정된 접근(controlled access)이 허용된 보안시스템(secure system)이며 또한 보안시스템으로 계속 작동하는지 여부를 검증(verification)하는 퍼스널 컴퓨터 시스템.

청구항 5. 제1항에 있어서, 선택카드를 수신하며, 상기 시스템프로세서와 작동적으로 연결되고, 상기 봉합체내에 위치하여 상기 봉합체의 개방 후에만 수동접근이 가능한, 최소한 하나의 I/O슬롯(I/O slot)을 더 포함하는 퍼스널 컴퓨터 시스템.

청구항 6. 제5항에 있어서, 상기 봉합체내에 설치되고 사용자가 제거할 수 없는, 대용량 저장장치(mass storage device)로서, 시스템 구획(system partition)을 구비하고 상기 시스템프로세서와 작동적으로 연결되어 프로그램 및 데이터를 저장하고 프로그램 및 데이터를 검색할 수 있는 대용량 저장장치와; 상기 대용량 저장장치의 상기 시스템 구획에 저장되고, 상기 퍼스널 컴퓨터 시스템의 통상의 사용자(normal user)나 인가되지 않은 사용자(unauthorized user)는 모두 접근이 불가능하여, 상기 슬롯에 설치된 임의의 선택 카드를 수용하도록 시스템 소유자나 인가된 사용자가 상기 퍼스널 컴퓨터 시스템을 선택적으로 인에이블 시키기 위한 시스템 구성 설정 유틸리티 프로그램(system configuration setting utility program)을 더 포함하는 퍼스널 컴퓨터 시스템.

도면

도면1

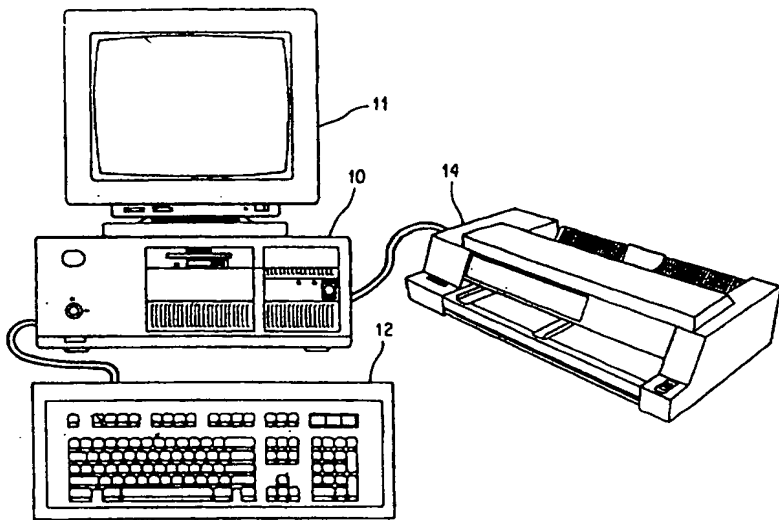


FIG. 2

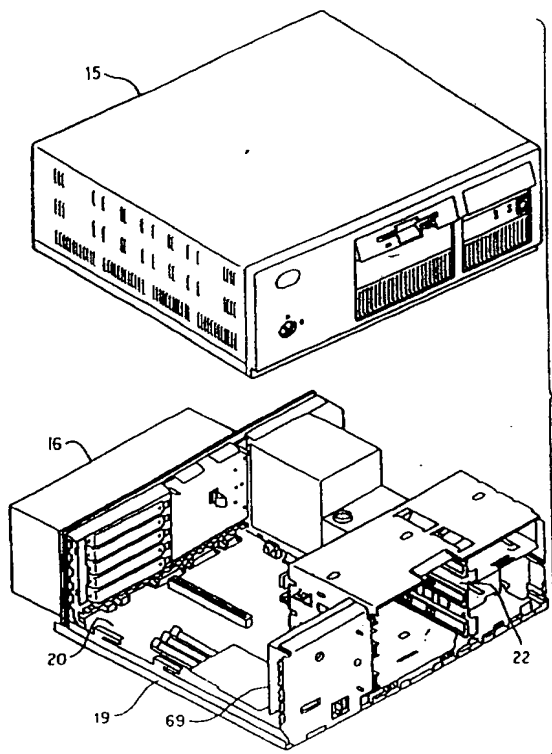


FIG. 3



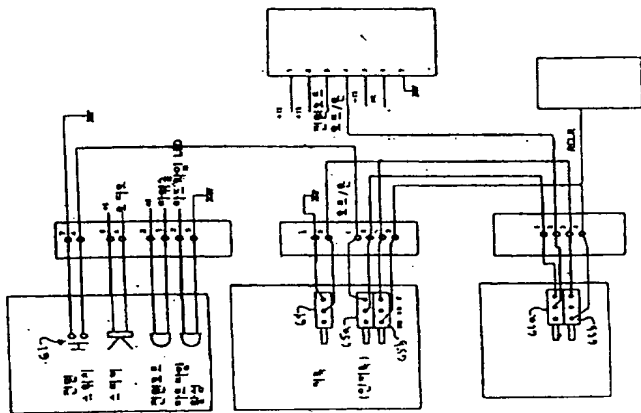


FIG 6

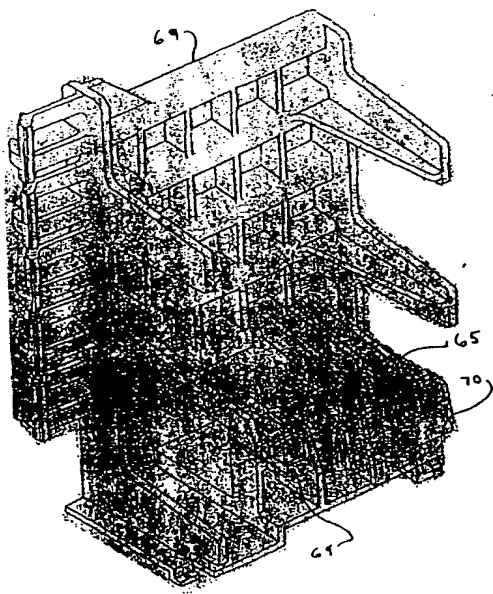
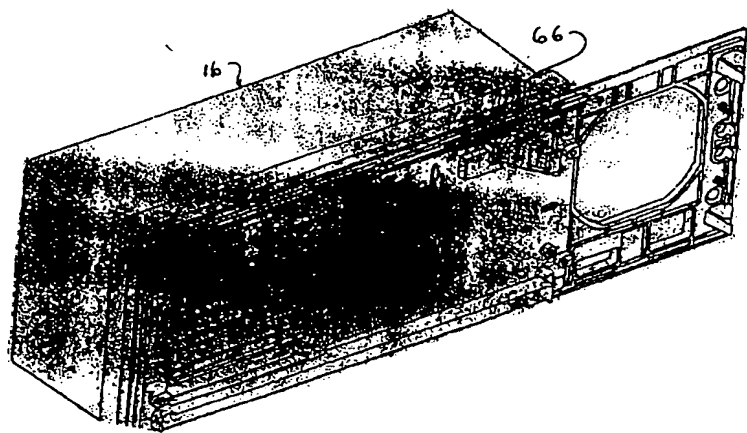


FIG 7



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☒ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.